PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/IB2004/001981	10.06.2004	21.06.2003

International Patent Classification (IPC) or both national classification and IPC
G06F7/72

Applicant
KONINKLIJKE PHILIPS ELECTRONICS N.V.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☒ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA"). However, this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of three months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:

European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Authorized Officer

Prins, L

Telephone No. +49 89 2399-7433

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IB2004/001981

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   ☐ This opinion has been established on the basis of a translation from the original language into the following language , which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material:

   ☐ a sequence listing

   ☐ table(s) related to the sequence listing

   b. format of material:

   ☐ in written format

   ☐ in computer readable form

   c. time of filing/furnishing:

   ☐ contained in the international application as filed.

   ☐ filed together with the international application in computer readable form.

   ☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non obvious), or to be industrially applicable have not been examined in respect of:

☐ the entire international application,

☒ claims Nos. 8,22,23

because:

☒ the said international application, or the said claims Nos. 1-2,5-7,9-10 relate to the following subject matter which does not require an international preliminary examination *(specify)*:

see separate sheet

☒ the description, claims or drawings *(indicate particular elements below)* or said claims Nos. 3,4,17,18 are so unclear that no meaningful opinion could be formed *(specify)*:

see separate sheet

☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.

☒ no international search report has been established for the whole application or for said claims Nos. 8,22,23

☐ the nucleotide and/or amino acid sequence listing does not comply with the standard provided for in Annex C of the Administrative Instructions in that:

the written form	☐	has not been furnished
	☐	does not comply with the standard
the computer readable form	☐	has not been furnished
	☐	does not comply with the standard

☐ the tables related to the nucleotide and/or amino acid sequence listing, if in computer readable form only, do not comply with the technical requirements provided for in Annex C-*bis* of the Administrative Instructions.

☐ See separate sheet for further details

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	11-14,16
	No:	Claims	15,19-21
Inventive step (IS)	Yes:	Claims	16
	No:	Claims	11-15,19-21
Industrial applicability (IA)	Yes:	Claims	11-16,19-21
	No:	Claims	

2. Citations and explanations

see separate sheet

1 Reference is made to the following document:

D1: LORENCZ R: "NEW ALGORITHM FOR CLASSICAL MODULAR INVERSE" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. INTERNATIONAL WORKSHOP, XX, XX, 13 August 2002 (2002-08-13), pages 57-70, XP001160521

Re Item III

2 No meaningful opinion can be formed on the novelty, inventive step, or industrial applicability of the subject-matter of claims 1-10, 17, 18, 22 and 23 (Article 34(4)(a)(ii)).

3 Claims 8, 22, 23 lack clarity (Article 6 PCT) to such an extent that a meaningful search of these claims could not be carried out (Art. 17(2)(a)(ii) PCT). The second line of claim 8 is missing, leaving no additional subject-matter that could be searched for this claim. Claims 22 and 23 both refer to the figures (PCT Guidelines I 5.10). Claims must be clear from the wording of the claim alone (PCT Guidelines I 5.31).

4 Claims 3 and 17 are unclear (Article 6 PCT) in that they refer to "the invariances" and "the invariance" respectively, without anticipants for these features. Such invariances are introduced in the following claims 4 and 18.

5 However, claims 4 and 18 are also unclear (Article 6 PCT) because they attempt to define the invention by a result to be achieved (PCT Guidelines I-5.35). Instead of the result ("having invariances: ..."), the steps, c.q., the means for performing the steps that provide for this result must explicitly be stated in the claim.

6 Claims 1-10 relate to purely abstract activities involving mathematical methods used in a cryptographic calculation. The claims do not specify any physical means to perform the steps of the methods. Consequently, they neither produce a concrete tangible result or cause an effect on a concrete physical entity. Lacking a manifest effect in the real world, such claims are considered purely abstract activities to be equated with mental acts within the meaning of Rule 39.1(i) PCT.

It is noted, that a technical character can be conferred to such purely abstract

activities by specifying concrete physical means used in performing such activities in the claim. The use of such means would ensure that an effect in the field of cryptography would be actually achieved and doesn't remain a purely abstract notion. The attention of the applicant is drawn to the fact that the application may not be amended in such a way that it contains subject-matter which extends beyond the content of the application as filed (Article 19(2) PCT).

Re Item V

7 Claim 11-14 lack inventive step (Article 33(3) PCT). The features of claim 1 to which these claims refer are well known from the binary Euclidean algorithm for computing the modular inverse, such as disclosed in D1 in algorithm I. Variable "v" is shifted on line 13 and then subtracted from larger variable "u" (line 15) on lines 14 and 16. The additional features of claims 11-14 relate to a software implementation of such an algorithm and its distribution. Software implementations of cryptographic algorithms and their distribution have been generally known in the field at the priority date so that these features cannot support an inventive step.

8 Claims 15 and 19-21 lack novelty (Article 33(2) PCT) over the well known binary Euclidean algorithm for computing the modular inverse, such as disclosed in D1 in algorithm I for the same reasons as shown under point 7. The abstract of D1 mentions that an apparatus ("hardware") may be used to implement the algorithm. Furthermore, the disclosed algorithm certainly operates with the Most Significant Words of the variables as specified in claim 21.

9 It is noted that, even if claims 1,3-10 were to be amended to refer to a method involving some technical means, such amended claims would not be novel over D1 for the same reasons as mentioned above.

10 Claims 2 and 16 could provide the basis for an inventive claim, provided that technical means are added to claim 2 and that both claims are amended so as to make it clear that the variables "being of the same degree" applies to the variable after shifting and a larger variable. In this respect, it was also noted that reference sign (S2) in present claim 1 does not refer to the step of "shifting" in figure 2 of the application.